Acceptable Use of Information Technology Resources Policy

POLICY TITLE
Acceptable Use of Information Technology Resources Policy

POLICY CATEGORY
Information Technology Services

PURPOSE
The purpose of this policy is to define the acceptable use of Springfield Technical Community College (STCC) applications, hardware, data, and other information technology resources and systems.

SCOPE
This policy applies to any person utilizing STCC information technology resources. The following persons (users) are authorized to use STCC information technology resources: (1) current faculty; (2) current staff; (3) current students; (4) authorized contractors or vendors; and (5) authorized visitors.

POLICY STATEMENT
Acceptable use of STCC information technology resources includes use for academic, educational or professional purposes that are directly related to official college business and in support of the college mission. Users are encouraged to utilize STCC information technology resources to the fullest extent in pursuit of the college's mission, goals and objectives. The college expects that these information technology resources are always used in a responsible manner and reserves the right to limit or remove access as required.

STCC electronic communications systems, including Internet, telephony, email, and messaging services are to be used primarily for college related purposes. Users shall have no expectation of privacy over any communication, transmission or work performed using or stored on college information technology resources. The college reserves the right to monitor any and all aspects of its information technology resources and to do so at any time, without notice and without the user's permission.

Springfield Technical Community College makes no warranties, expressed or implied, for the information technology resources it provides. STCC will not be responsible for any damages a user may suffer, including loss of data, undelivered messages or content or service interruptions. STCC denies any responsibility for the accuracy or quality of information obtained through its information technology resources. The college is a "carrier" of information through electronic channels rather than a "publisher" of information. With the exception of official college publications or legitimate business communications through internal processes, the college is not to be expected to be aware of, or responsible for materials or communications.

Uses of Technology

1. Access – All access to STCC applications, systems and hardware shall be authorized and approved. Any access not explicitly authorized and approved is prohibited. Access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate need for such access. The level of access granted, and privileges assigned, shall be limited to the minimum required to perform assigned duties or to access appropriate systems or services.
2. Remote Access – is authorized for only those users with an approved business or academic use. Users who have been approved for remote access are responsible for adhering to the requirements defined in the **Remote Access Policy.**
3. Media – users shall not use media, such as flash drives or portable hard drives, until they have been scanned for viruses, spyware, malware or other similar threats to the security or functionality of STCC information technology resources.
4. Data Encryption and Storage – confidential and/or personally identifiable information (PII) must be protected by encryption. Encryption methods that have been approved and implemented by Information Technology Services should be used in all cases. Encryption must be utilized when sending any login credentials or other sensitive or confidential information. Users who are unfamiliar with using approved encryption technologies should seek guidance from the IT Help Desk.
5. Cloud Computing and Storage – advances in cloud computing offer convenient technology solutions such as data storage and connectivity. Data placed on any cloud computing storage solution must adhere to the same policies as data stored on STCC internal technology resources and must be approved by the Information Technology Department prior to any use.

Unacceptable use of technology includes, but are not limited to:

- Activities that violate local, state or federal laws and/or regulations;
- Excessive, unreasonable or unauthorized personal use;
- Storing, sending, or forwarding emails that contain libelous, defamatory, obscene, threatening or harassing content;
- Infringing on intellectual property rights;
- Using systems for commercial purposes;
- Activities that attempt to circumvent or disable protection mechanisms that have been put in place by the college;
- Utilize external media on the network that may contain viruses or malware.

Computer Virus and Malware Protection

It is important that users take care to avoid compromising the security of the STCC network. Users shall exercise reasonable precautions to prevent the introduction of a computer virus or other malware into the STCC network. Virus scanning software is installed on all STCC systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Users must scan portable media devices for viruses and malware before using them to ensure that they have not been infected. If users are unsure of how to utilize virus and malware scanning tools, they should contact the IT Help Desk for additional information.

Messaging Technologies

Use of email and other messaging technologies shall never be used to transmit Personally Identifiable Information (PII) in an unencrypted format. Users must pay additional attention to email content and senders and must not open email attachments from unrecognized or suspicious senders. If there are questions about the security of an email, email attachment, or messaging technology users should contact the college IT Help Desk. For additional information on the use of email and messaging technologies at STCC, consult the **Electronic Communications Policy**.

Definition of Personally Identifiable Information (PII)

Personally Identifiable Information is any information about an individual generated, received, and/or stored by STCC that could be used to distinguish or trace a person's identity. This information also includes numbers that *directly* and uniquely identify an individual such as name, social security numbers or biometric information or any *indirec*t information that can be linked through the sum of its parts to an individual, such as medical, educational, or stored financial information. College personnel and/or authorized contractors or vendors may collect and/or store PII where necessary in order to perform a legitimate business-related activity and when no reasonable alternative exists. All such collection and/or storage of PII shall be performed in accordance with state and federal law, including, the Family Educational Rights and Privacy Act (FERPA).

Where no legitimate business-related activity exists, no user may collect or store the following PII:

- Social Security Number (SSN), passport number, driver's license number or state issued identification card numbers;
- Date of birth, place of birth or mother's maiden name;
- Credit card numbers, debit card numbers, bank account info or income tax records;
- Address information, such as street address or email address;
- Personal characteristics, including photographic image (especially the face or other identifying characteristic);
- Information about a person, including student 900 numbers or employee ID numbers, that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, educational information or financial information).

Network Access

STCC network access is restricted to authorized users only. Users must have a domain user identity to access the network.

Wireless Access

To improve mobility, connectivity and collaboration opportunities, STCC provides three wireless (Wi-Fi) networks; 'facstaff' 'student' and 'guest' at certain locations. Users must be aware that not all internal applications will be available through the guest Wi-Fi or from personal devices. Personnel who wish to use wireless connections to conduct STCC business will be required to connect to the secured network with an STCC approved device. Non-STCC devices must use the ‘guest’ wireless network.

Remote Access

Users who access the STCC network remotely must be authenticated prior to establishing a network connection and comply with the **Remote Access Policy**.

Incident Response

STCC IT staff will respond to all information technology security related incidents, such as computer virus infections. To effectively respond to these events, the ITS staff relies on timely information and reporting from users. Subsequently, users are required to contact the STCC IT Help Desk if they:

- Observe unauthorized or suspicious activity;
- Know or suspect that a violation of this Policy has or is about to occur.

Password Use

Many of STCC information technology resources require the use of a unique user account and password. It is important for college users to create strong passwords and protect these passwords. Users must never share their passwords with anyone else, must maintain privacy of their password, and must promptly notify IT personnel if they suspect their passwords have been compromised. For additional information on password creation, use and protection, refer to the **Password Policy**.

Physical and Environmental Security

Assistance from users is required to ensure a physically and environmentally secure working environment. Users are required to be aware of locking and access restriction mechanisms and must immediately report any unidentified or unescorted individuals within restricted areas of the college. Users who leave their devices unattended must log off or lock the system before leaving.

Problem Management

Users are required to report problems or issues discovered with STCC information technology resources to the IT Help Desk immediately following discovery.

Information Security Awareness

College personnel may be required to complete annual information security awareness training upon hire and at least annually thereafter according to the **Information Security Awareness Training Policy.**

ENFORCEMENT

Any user found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment, expulsion from the college or discontinuation of the business relationship. Depending upon the nature of the violation of this policy, a user may also be subject to civil liability and/or criminal prosecution.

REVISION HISTORY

This section contains information on the approval and revision history for this policy.

Version Number	Issued Date	Approval	Description of Changes
1.0	3/2016	Massachusetts CIO Council	Development and adoption of collaborative and standardized IT policies
1.0	7/2016	Massachusetts Community College Counsel's Office	Recommendation on contents provided by college counsel
2.0	8/2021	Trustee Internal/External Committee	Policy revision and review
2.0	8/2021	College Adoption	Revisions implemented